

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)An Apple iPhone X (black with clear case), assigned call number (317)
922-4664, subscribed to by Jeffrey ROACH, with International Mobile
Subscriber Identity 3104 1001 1852 199, currently located at the
SSA-OIG Philadelphia Field Office, assigned evidence number E-18-0001

Case No. 18-1346M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, location to be searched, incorporated by reference

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated by reference

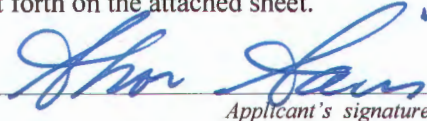
The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. sections 1343,
1028A, 513(a) and 371Offense Description
wire fraud, aggravated identity theft, uttering counterfeited securities of an
organization in interstate commerce, and conspiracy to commit wire fraud and
utter counterfeited securitiesThe application is based on these facts:
See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Shon Sain, Special Agent, SSA OIG

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/22/2018

City and state: Philadelphia PA



Judge's signature

United States Magistrate Judge Carol Sandra Moore Wells

Printed name and title

ATTACHMENT A:

ITEM TO BE SEARCHED

An Apple iPhone X (black with clear case), assigned call number (317) 922-4664, subscribed to by Jeffrey ROACH, with International Mobile Subscriber Identity 3104 1001 1852 199, assigned evidence number E-18-0001 and currently located at the SSA-OIG Philadelphia Field Office.

ATTACHMENT B: ITEMS TO BE SEIZED

1. All records that relate to violations of 18 U.S.C. §§ 513(a) (uttering counterfeit securities), 1343 (wire fraud), 371 (conspiracy), and 1028A (aggravated identity theft), including:
 - a. Documents in electronic form, including correspondence, records, opened or unopened emails, text messages, voicemail messages, call logs, chat logs, internet history, GPS data and map history pertaining to the planning or commission of the criminal scheme described in this application; and the distribution, expenditure or location of proceeds of the crimes.
 - b. Photographs relating to the planning or commission of the crimes, including photographs of Jeffrey ROACH and his co-conspirators/accomplices; the victims of their frauds; clothing worn during the crimes; and other items used during the crimes; the proceeds of their crimes; and items purchased with the proceeds of the crimes.
 - c. Address books and calendars.
2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including, but not limited to the following:
 - a. Forms of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

- b. Data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system, including any and all electronic data which can be collected, analyzed, created, displayed, converted, stored, concealed, or transmitted, or similar computer impulses or data.
 - c. Stored electronic information and communications, including but not limited to, telephone or address directory entries consisting of names, addresses and telephone numbers; logs of telephone numbers dialed, telephone numbers of missed calls, and telephone numbers of incoming calls; schedule entries; stored memoranda; stored text messages; stored photographs; store audio; and stored video.
- 3. Evidence and contents of logs and files on the device, such as those generated by the device's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the device at the time any actions relating to the above offenses were taken.

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, SHON SAIN, being duly sworn, state as follows:

1. I am a Special Agent ("SA") of the Social Security Administration, Office of the Inspector General ("SSA-OIG") and have been so employed since November 2007. Prior to my current employment, I was a Special Agent of the United States Secret Service ("USSS") from April 2000 to November 2007. I am currently assigned to the Philadelphia Field Office, and I conduct criminal investigations of federal law, including cases involving misuse of Social Security numbers, in violation of 42 U.S.C. § 408, and theft of government funds, wire fraud, identity theft, bank fraud and access device fraud, in violation of 18 U.S.C. §§ 641, 1028(a), 1028A, 1343, 1344 and 1029, respectively, among other financial crimes. I have also completed hundreds of hours of training, conferences and workshops, on investigating the above-mentioned crimes. Your affiant has also led, coordinated, and assisted in the execution of numerous arrest warrants relating to these crimes.

2. I am the SSA-OIG's case agent in a case entitled *United States v. Ahmad Becoate et al.*, Criminal No. 18-291-1 through 6. I make this affidavit in support of an application for a warrant to search a cellular telephone, more specifically, an Apple iPhone X cell phone, black in color with a clear protective case, assigned call number (317) 922-4664, subscribed to by Jeffrey ROACH, with International Mobile Subscriber Identity 3104 1001 1852 199 (the "Subject Cellular Telephone"). As set out below, your affiant and the case agent from the United States Postal Inspection Service ("USPIS"), Samuel Bracken, seized the Subject Cellular Telephone from the person of Jeffrey Roach on August 14, 2018 when we arrested Roach that day in Owings Mill Maryland, near Baltimore. The Subject Cellular Telephone is currently located at

the SSA-OIG Philadelphia Field Office, where it is secured in an evidence locker, assigned property evidence number E-18-0001.

3. On July 10, 2018, a grand jury sitting in this District returned an indictment entitled *United States v. Becoate, et al.*, filed under Criminal No. 18-291-01 through 06 (“the indictment”). A copy of the indictment is attached as Exhibit C to this Affidavit. The indictment, unsealed August 14, 2018, alleges that beginning no later than June 2016 and continuing until at least May 2018, Becoate, ROACH and others conspired and schemed to present thousands of counterfeit payroll checks, with a face value of more than \$700,000, at Walmart stores located across the United States. According to the indictment, Becoate, Roach and others carried out the scheme by using the personal identifying information, including social security numbers, of thousands of innocent persons. The indictment charges further that these actions violated Title 18, United States Code, Section 513(a) (uttering counterfeit securities); Title 18, United States Code, Section 1343 (wire fraud); Title 18, United States Code, Section 371 (conspiracy to commit wire fraud and utter counterfeit securities); Title 18, United States Code, Section 1028A (aggravated identity theft); and Title 42, United States Code, Section 408(a)(7). There is also probable cause to search the cellular telephone described in Attachment A for evidence and instrumentalities of these crimes as further described in Attachment B.

4. The facts in this affidavit come from my personal observations, my training and experience, review of documents and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

Probable Cause

5. Along with my co-case agents, who are Special Agents of the United States Secret Service (“USSS”) and the USPIS, I am investigating the activities of a group of individuals who have been engaged in a nationwide identity theft and counterfeit check cashing scheme since at least June 2016, which activity, at least by several subjects, has continued until July 2018.

6. During this investigation, your affiant learned from Walmart representatives that at some Walmart locations, Walmart permitted customers to cash payroll checks. When a customer presented a payroll check to a Walmart employee for cashing, the customer was required to enter his or her social security number (“SSN”) into a keypad. The Walmart employee scanned the check through a check reader. Certain information including the account number of the bank account on which the payroll check was drawn; the drawee bank’s routing number; and the SSN provided by the customer was transmitted via interstate wire transmission from the Walmart store’s computer system to the computer servers of a contractor for Walmart. The contractor had computer servers in Chicago, Illinois and St. Petersburg, Florida. The contractor analyzed the data provided by the check and the Walmart customer, then transmitted an interstate wire communication from its computer servers back to the Walmart store, recommending acceptance or declination of the payroll check.

7. As part of the investigation my co-case agents and I interviewed a co-conspirator of Jeffrey ROACH (the “Cooperating Defendant”), who was charged in the indictment and has signed a cooperation plea agreement with the United States government. The Cooperating Defendant hopes to obtain a lower sentence in return for his/her cooperation. The Cooperating Defendant stated that he/she and his/her co-conspirators obtained from what the Cooperating Defendant termed a “Russian website” the personal identifying information (“PII”) of innocent

persons to use as payees on counterfeit checks that members of the group manufactured. The Cooperating Defendant also stated that he/she and other members of the group used their cellular phones to communicate with each other; to store PII, including social security numbers, for use when cashing counterfeit checks at the Walmart stores; and to send each other fraudulent drivers' license information to use in cashing the counterfeit checks. Analysis of the call records of the Subject Cellular Telephone shows over 500 calls between the Subject Cellular Telephone and the Cooperating Defendant's cellular telephone between January 27, 2017 and February 11, 2018. I know from my investigation that the Cooperating Defendant was taken into custody on other federal charges on or about February 18, 2018, and has been in custody since that date.

8. During the investigation, Walmart supplied the investigating agents with a large number of digital recordings showing the conspirators, including Jeffrey ROACH, presenting counterfeit checks at various Walmart locations. The Cooperating Defendant identified a number of photographs taken from the digital recordings as depicting ROACH. On some of the digital recordings, ROACH was seen at the customer service counter looking at his cellular telephone while using the keypad. Based on these digital recordings and the Cooperating Defendant's account of how he/she and the other members of the group used their cellular telephones in the scheme, your affiant believes that ROACH has been using a cellular telephone (that is, since January 26, 2017, a cellular telephone assigned call number (317) 922-4664) at Walmart stores to access stolen social security numbers in order to cash counterfeit checks.

9. Also as part of the investigation, my co-case agents and I obtained eight email search warrants on eight email accounts, including two email accounts used by Jeffrey ROACH. For one of the two email accounts used by ROACH, assigned call number (317) 922-4664 -- the number of the Subject Cellular Telephone -- was the registered telephone number on the email

account. Analysis of the material obtained through the searches of the email accounts of ROACH and others showed that the accounts contained PII, including PII that had been used in passing counterfeit checks at Walmart locations, as confirmed by review of Walmart records.

10. Investigation has shown further that during the conspiracy period, starting as early as September 28, 2017, and continuing until approximately June 15, 2018, the lead defendant on the indictment, Ahmad Becoate, used a cellular telephone with the assigned call number (202) 255-5236 ("Becoate's cellular telephone"). Call records for Becoate's cellular telephone show that between September 28, 2017 and June 15, 2018, Becoate's cellular telephone was used to make and receive over 1,000 calls with the Subject Cellular Telephone. The investigation has shown further that during the conspiracy period, starting as early as January 26, 2017, and continuing until approximately June 15, 2018, Jeffrey ROACH used a cellular telephone that was assigned call number (317) 922-4664. As stated above in paragraph 7, call records of the Subject Cellular Telephone also show calls to and from the Cooperating Defendant's cellular telephone.

11. In addition, based on statements made by the Cooperating Defendant, summarized above at paragraph 7, your affiant believes that ROACH, like the Cooperating Defendant, has also used the Subject Cellular Telephone to access stolen social security numbers at Walmart stores in order to cash counterfeit checks, and to send and receive emails and/or text messages containing fraudulent drivers' license information and PII of innocent persons.

12. Photographic evidence provided by Walmart investigators shows that as recently as June 19, 2018, Jeffrey ROACH passed a counterfeit payroll check at a Walmart in Las Vegas, Nevada. Based on previous identifications of ROACH made by the Cooperating Defendant and my familiarity with ROACH's appearance gained through investigation of this case, your affiant

has identified the surveillance photographs of the individual in the Las Vegas Nevada Walmart on June 19, 2018, as Jeffrey ROACH.

13. On August 2, 2018, an application for a “pen register” and “trap and trace” data for the Subject Cellular Telephone, as well as a second telephone, was approved in the Eastern District of Pennsylvania.

14. On August 14, 2018, USPIS inspectors and agents of SSA-OIG established physical surveillance of Jeffrey ROACH in Owings Mills, MD. During the surveillance, your affiant saw ROACH walking towards his vehicle using the Subject Cellular Telephone. ROACH was arrested without incident pursuant to the warrant issued in connection with the indictment. During the arrest, the arresting agents seized the Subject Cellular Telephone from the person of ROACH, placed it in “airplane mode,” and secured the Subject Cellular Telephone pending application to this Court for a search warrant.

15. The Subject Cellular Telephone is a cellular telephone. Based on my training and experience, as well as the training and experience of other agents, a cellular telephone (also called a mobile telephone or wireless telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called “cells,” enabling communication with other cellular telephones or traditional “land line” telephones. A cellular telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic

“address books;” sending, receiving, and storing email, voice messages and text messages¹; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device and for mapping and navigation features. Based on my training and experience, I am aware that people who engage in illegal activities such as counterfeit check fraud have been known to use some or all of these features in furtherance of their illegal activities.

16. Furthermore, based on my training and experience, I know that electronic devices such as cellular telephones can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensic tools. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

17. Based on my training and experience, I know that people who engage in these types of crimes will often communicate with their coconspirators and/or accomplices by way of cellular telephone (including via text message) before, during, and after passing counterfeit checks. Further, I am aware that people who engage in crimes will often use the internet (including on their cell phones) to search for information about their intended victims, such as the locations and hours of businesses. Further, I am aware that people who engage in these types

¹ Based on my training and experience, I am aware that, among the services commonly offered by cellular telephone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber’s phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as “Short Message Service” (“SMS”) or “Multimedia Messaging Service” (“MMS”), and is often referred to generically as “text messaging” or “wireless messaging” (collectively referred to in this affidavit as “text messages”).

of crimes often possess photographs (including in their phones) of themselves and their co-conspirators/accomplices; the victims of their scheme; clothing worn during the crime; the proceeds of their fraud schemes; and items purchased with the proceeds of the crime. I also know from my training and experience that criminals, including those who engage in this type of crime, often have multiple telephones to facilitate their commission of illegal activities while attempting to thwart identification by law enforcement through the use of multiple phones or "burner" phones which cannot be traced back to an individual.

18. Evidence of calls and text messages made by, to and among the members of this conspiracy in the course of the events described in this Affidavit are expected to be disclosed by the requested searches. Among other reasons cited herein, a search of the Subject Cellular Telephone is required to determine the telephone number assigned to the device, thus enabling its further identification as the phone used by Jeffrey ROACH, and which communicated with telephones used by other co-conspirators, as a part of this conspiracy. Also, by analyzing call activity, agents may be able to determine where other accomplices were in the area, and if there were communications between accomplices during the commission of the crimes.

19. This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

1. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

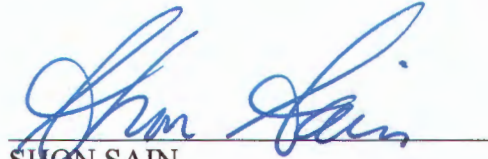
2. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
3. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
4. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
5. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

20. Searching for the evidence described in Attachment B to the Subject Cellular Telephone warrant application may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not

yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit the examination of the device using whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.


21. Based on the foregoing, there is probable cause to believe that Jeffrey ROACH has committed violations of 18 U.S.C. §§ 513(a) (uttering counterfeit securities), 1343, (wire fraud), 371 (conspiracy), and 1028A (aggravated identity theft), among other offenses, and that evidence and instrumentalities of these violations exists in the location described above.

Accordingly, your affiant requests that this Court issue a warrant to search the Subject Cellular Telephone, more fully described in Attachment A, for the evidence and instrumentalities of these crimes, described in Attachment B.



SHON SAIN
Special Agent
Social Security Administration, Office
of Inspector General

Sworn to before me
this 22nd day of August 2018


HONORABLE CAROL SANDRA MOORE WELLS
United States Magistrate Judge

ATTACHMENT A:

ITEM TO BE SEARCHED

An Apple iPhone X (black with clear case), assigned call number (317) 922-4664, subscribed to by Jeffrey ROACH, with International Mobile Subscriber Identity 3104 1001 1852 199, assigned evidence number E-18-0001 and currently located at the SSA-OIG Philadelphia Field Office.

ATTACHMENT B: ITEMS TO BE SEIZED

1. All records that relate to violations of 18 U.S.C. §§ 513(a) (uttering counterfeit securities), 1343 (wire fraud), 371 (conspiracy), and 1028A (aggravated identity theft), including:
 - a. Documents in electronic form, including correspondence, records, opened or unopened emails, text messages, voicemail messages, call logs, chat logs, internet history, GPS data and map history pertaining to the planning or commission of the criminal scheme described in this application; and the distribution, expenditure or location of proceeds of the crimes.
 - b. Photographs relating to the planning or commission of the crimes, including photographs of Jeffrey ROACH and his co-conspirators/accomplices; the victims of their frauds; clothing worn during the crimes; and other items used during the crimes; the proceeds of their crimes; and items purchased with the proceeds of the crimes.
 - c. Address books and calendars.
2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including, but not limited to the following:
 - a. Forms of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

- b. Data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system, including any and all electronic data which can be collected, analyzed, created, displayed, converted, stored, concealed, or transmitted, or similar computer impulses or data.
 - c. Stored electronic information and communications, including but not limited to, telephone or address directory entries consisting of names, addresses and telephone numbers; logs of telephone numbers dialed, telephone numbers of missed calls, and telephone numbers of incoming calls; schedule entries; stored memoranda; stored text messages; stored photographs; store audio; and stored video.
- 3. Evidence and contents of logs and files on the device, such as those generated by the device's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the device at the time any actions relating to the above offenses were taken.

ATTACHMENT A:

ITEM TO BE SEARCHED

An Apple iPhone X (black with clear case), assigned call number (317) 922-4664, subscribed to by Jeffrey ROACH, with International Mobile Subscriber Identity 3104 1001 1852 199, assigned evidence number E-18-0001 and currently located at the SSA-OIG Philadelphia Field Office.

EXHIBIT C